ANALISIS KLASIFIKASI SERANGAN DENIAL OF SERVICE (DOS) DENGAN METODE DECISION TREE MENGGUNAKAN WEKA (WAIKATO ENVIRONMENT FOR KNOWLADGE ANALYSIS)

SKRIPSI

Oleh :

ACHMAD ZUBAIRI MAS'UD
1034010070

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL
"VETERAN" JAWA TIMUR
2014

SKRIPSI

ALISIS KLASIFIKASI SERANGAN DENIAL OF SERVICE (DOS) DENGAN METODE DECISION TREE MENGGUNAKAN WEKA (WAIKATO ENVIRONMENT FOR KNOWLADGE ANALYSIS)

Disusun Oleh :

ACHMAD ZUBAIRI MAS'UD

1034010070

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Pada Tanggal : 23 Desember 2014

Pembimbing :

Budi Nugroho, S.Kom, M.Kom.
NPT. 3 8009 050 205 1

I Made Suartana, S.Kom, M.Kom.
NIP. 113111984

Tim Penguji :

1. Rizky Parlika, S.Kom, M.Kom.
NPT. 3 8405 070 219 1

2. Basuki Rahmat, S.Si., MT.
NPT. 3 6907 060 209 1

3. I Made Suartana, S.Kom, M.Kom.
NIP. 113111984

Mengetahui
Dekan Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Surabaya

Ir. Sutiyono, MT
NIP. 19600713 198703 1001

LEMBAR PENGESAHAN

LISIS KLASIFIKASI SERANGAN DENIAL OF SERVICE (DOS) ENGAN METODE DECISION TREE MENGGUNAKAN WEKA (WAIKATO ENVIRONMENT FOR KNOWLADGE ANALYSIS)

Oleh :

ACHMAD ZUBAIRI MAS'UD

1034010070

Telah disetujui mengikuti Ujian Negara Lisan
Gelombang II Tahun Akademik 2014 / 2015

Menyetujui,

Pembimbing I	Pembimbing II
Budi Nugroho, S.Kom, M.Kom.	I Made Suartana, S.Kom, M.Kom.
NPT. 3 8009 050 205 1	NIP. 113111984

Mengetahui,
Ketua Program Studi Teknik Informatika
Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur

Budi Nugroho, S.Kom, M.Kom.
NPT. 3 8009 050 205 1

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAWA TIMUR
FAKULTAS TEKNOLOGI INDUSTRI
Jl. Rungkut Madya Gunung Anyar Surabaya 60294 Tlp. (031) 8706369, 8783189
Fax. (031) 8706372 Website. www.upnjatim.ac.id

KETERANGAN REVISI

Kami yang bertanda tangan di bawah ini menyatakan bahwa mahasiswa berikut :

Nama : Achmad Zubairi Mas'ud

Npm : 1034010070

Program Studi : Teknik Informatika

Telah mengerjakan REVISI SKRIPSI Ujian Lisan Gelombang VI. TH, 2014
Dengan Judul :

ANALISIS KLASIFIKASI SERANGAN DENIAL OF SERVICE (DOS) DENGAN METODE DECISION TREE MENGGUNAKAN WEKA (WAIKATO ENVIRONMENT FOR KNOWLADGE ANALYSIS)

Surabaya, 2 Januari 2014

Dosen penguji yang memeriksa revisi

1. Rizky Parlika,S.Kom,M.Kom,
   NPT : 3 8405 070 219 1
2. Basuki Rahmat , S,SI,MT
   NPT : 3 6907 060 209 1
3. I.Made Suartana S.Kom,M.Kom
   NIP : 113111984

Mengetahui,

Pembimbing Utama

Budi Nugroho ,S.Kom,M.Kom.
NPT : 3 8009 050 205 1

ANALISIS KLASIFIKASI SERANGAN DENIAL OF SERVICE (DOS) DENGAN METODE DECISION TREE MENGGUNAKAN WEKA (WAIKATO ENVIRONMENT FOR KNOWLADGE ANALYSIS)

Nama : Achmad Zubairi Mas'ud
Dosen Pembimbing 1 : Budi Nugroho, S.Kom. M.Kom
Dosen Pembimbing 2 : I Made Suartana, S.Kom. M.Kom

ABSTRAK

Dengan adanya sistem komputer berbasis jaringan yang sekarang berperan penting dalam kehidupan masyarakat modern sekarang ini, telah menjadi sasaran kejahatan dalam dunia cyber yang dilakukan oleh penyusup atau hacker, dan jumlah serangan jaringan saat ini yang terus meningkat, maka dibutuhkan Intrusion Detection System (IDS) yang mampu memantau dan mendeteksi gangguan atau intrusi pada seluruh sistem.

Agar sebuah Intrusion Detection System dapat mendeteksi jenis serangan baru, salah satu teknik yang bisa digunakan adalah dengan teknik data mining dalam IDS. Dan dalam mendeteksi suatu intrusi dibutuhkan salah satu metode dalam data mining yang mampu mengklasifikasikan sebuah serangan dengan baik yaitu decision tree.

Dan dalam tugas akhir ini dilakukan klasifikasi terhadap dataset yang dibuat dari proses data log dengan menggunakan metode decision tree dan dataset KDD CUP 1999 sebagai data training. Dan hasil dari klasifikasi pada data test menunjukkan bahwa metode decision tree cukup akurat dalam mengklasifikasikan serangan terhadap data test yang dibuat dengan rata-rata hasil keseluruhan klasifikasi pada data test sebesar 91.2% untuk class yang diprediksi dengan tepat.

Keyword : Intrusion Detection System, Data Mining, Decision Tree, WEKA

KATA PENGANTAR

Pertama kali ijinkanlah kami mengucapkan puja dan puji syukur ke Hadirat Tuhan Yang Maha Kuasa atas selesainya pembuatan laporan Tugas Akhir (TA) ini di Universitas Pembangunan Nasional "Veteran" Jawa Timur dengan judul "Analisis Klasifikasi Serangan Denial of Service (DOS) Dengan Metode Decision Tree Menggunakan WEKA (Waikato Environment for Knowladge Analysis).

Penulis menyadari, Bahwa laporan Tugas Akhir ini belum sempurna dan masih banyak kekurangan. Oleh karena itu penulis sangat mengharapkan kritik dan saran dalam memperbaiki laporan ini agar menjadi lebih baik lagi.

Akhir kata penulis berharap agar Tugas Akhir ini yang telah disusun sesuai dengan kemampuan dan pengentahuan yang sangat terbatas ini dapat bermanfaat bagi pihak yang membutuhkan.

Surabaya, 23 Desember 2014

Penulis

UCAPAN TERIMA KASIH

Puji syukur ke hadirat Allah SWT yang telah memberikan rahmat dan karunia-Nya, sehingga dapat terselesaikannya Tugas Akhir ini.

Dengan selesainya tugas akhir ini tidak terlepas dari bantuan banyak pihak yang telah memberikan masukan-masukan. Untuk itu penyusun mengucapkan terima kasih sebagai perwujudan rasa syukur atas terselesaikannya tugas akhir ini dengan lancar. Ucapan terima kasih ini saya tujukan kepada :

1. Bapak Prof. Dr. Ir. Teguh Soedarto, MP selaku Rektor Universitas Pembangunan Nasional “Veteran” Jawa Timur.
2. Bapak Ir. Sutiyono, MT selaku Dekan Fakultas Teknologi Industri UPN “Veteran” Jawa Timur.
3. Budi Nugroho S.Kom, M.Kom selaku Ketua Jurusan Teknik Informatika UPN “Veteran” Jawa Timur dan dosen pembimbing I pada Tugas Akhir ini, yang telah banyak memberikan petunjuk, masukan, bimbingan, dorongan serta kritik yang bermanfaat sejak awal hingga terselesainya Tugas Akhir ini.
4. I Made Suartana, S.Kom, M.Kom selaku dosen pembimbing II yang telah banyak memberikan petunjuk, masukan serta kritik yang bermanfaat hingga terselesainya Skripsi ini.
5. Terima kasih buat Ibu, Ayah dan Kakak-Kakak tercinta yang telah memberi semangat, dorongan dan do’a yang tiada henti-hentinya hingga dapat terselesaikannya tugas akhir ini.

6. Terima kasih buat sahabat saya Rendy, Rizal, Agung, Bagus, Handy, Adit, Indra, Irwan yang telah berjuang bersama sampai akhir perkuliahan dan telah memberikan semangat untuk menyelesaikannya dan yang selalu ada disaat suka dan duka saat mengerjakan Tugas Akhir ini.
7. Terimakasih kepada comunitas Blacklist yang telah memberikan banyak teman selama kuliah.
8. Serta orang-orang yang tidak dapat saya sebutkan satu persatu namanya. Terimakasih atas bantuannya semoga Allah SWT yang membalas semua kebaikan dan bantuan tersebut.

Surabaya, 23 Desember 2014

Penulis

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Dengan adanya sistem komputer berbasis jaringan yang sekarang berperan penting dalam kehidupan masyarakat modern sekarang ini, telah menjadi sasaran kejahatan dalam dunia cyber yang dilakukan oleh penyusup atau hacker, dan jumlah serangan jaringan saat ini yang terus meningkat, maka dibutuhkan Intrusion Detection System (IDS) yang mampu memantau dan mendeteksi gangguan atau intrusi pada seluruh sistem.

Intrusion Detection System sendiri adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Namun Kebanyakan IDS mendeteksi serangan dengan menganalisis informasi dari sebuah host tunggal pada banyak lokasi di seluruh jaringan. Akibatnya, komponen IDS melewatkan komunikasi antara satu sama lain. Fakta ini menghambat kemampuan untuk mendeteksi serangan terdistribusi dengan skala besar.

Untuk mengatasi masalah tersebut dibutuhkan sebuah agent dalam IDS. agent adalah sebuah program yang dapat bergerak secara individu atau otoritas organisasi, bekerja secara mandiri dalam mencapai tujuan, dan berinteraksi dengan agent lainnya. Dengan adanya agent yang memiliki kemampuan bergerak dari satu host ke host yang lain dan saling berinteraksi dengan agent yang lain, maka sistem dapat memproses informasi dari masing-masing host yang di pantau.

Agar IDS dapat mendeteksi jenis serangan baru, salah satu teknik yang bisa digunakan adalah dengan teknik data mining dalam IDS. Data mining merupakan teknik yang berkembang dalam dunia pengolahan data saat ini, tujuan data mining adalah mengekstrasi informasi secara otomatis dari sebuah database yang besar. Selain itu, dengan menggunakan integrasi dari kedua metodologi agent dan teknik data mining pada IDS, dapat meningkatkan kinerja dari IDS terdistribusi, mendeteksi serangan yang diketahui dan tidak diketahui dengan tingkat akurasi yang tinggi dalam lingkungan terdistribusi. Serta dalam teknik data mining, pola (atau tanda tangan) dari aktivitas normal dan abnormal (intrusi) dapat dibuat secara otomatis. Hal ini juga memungkinkan untuk memperkenalkan jenis serangan baru melalui proses pembelajaran tambahan. Akibatnya, semakin banyak serangan dapat dideteksi dengan benar.

Pada penelitian sebelumnya yang dilakukan oleh O.Oriola ,A.B. Adeyemo & A.B.C. Robert. Mereka menggabungkan antara agent dan data mining untuk mendeteksi intrusi yang ada dalam jaringan dan juga menggunakan hasil dari analisa dataset KDD CUP 1999 untuk membangun sebuah Distibuted Intrusion Detection System (DIDS) (O.Oriola, A.B. Adeyemo & A.B.C. Robert,"Distributed Intrusion Detection System Using P2P Agent Mining Scheme").

Dalam tugas akhir ini akan memproses data log yang dihasilkan oleh agent mining yang akan digunakan sebagai dataset dalam melakukan klasifikasi serangan dengan metode decision tree. Dalam proses klasifikasi akan menggunakan dataset KDD CUP 1999 yang merupakan kumpulan data yang digunakan untuk The Third International Knowledge Discovery and Data mining Tools Competition sebagai data training dan dataset dari data log agent mining

yang disimulasikan menggunakan TCPdump sebagai data test. Dan untuk melakukan klasifikasi akan menggunakan perangkat lunak WEKA (Waikato Environment for Knowladge Analysis) untuk mengetahui tingkat keakuratan metode decision tree dalam mengklasifikasikan sebuah serangan .

1.2 RUMUSAN MASALAH

Adapun rumusan masalah yang akan di bahas dalam tugas akhir ini :

a. Bagaimana menangkap paket-paket data dari serangan yang dilakukan?
b. Bagaimana memproses hasil data log mentah TCPdump menjadi sebuah dataset data mining?
c. Bagaimana membuat model klasifikasi dari data training KDD CUP 1999?
d. Bagaimana cara melakukan klasifikasi untuk menetukan jenis serangan pada dataset yang dibuat?
e. Bagaimana cara menganalisa hasil klasifikasi dari dataset yang dibuat?

1.3 BATASAN MASALAH

Batasan masalah yang terdapat pada tugas akhir ini adalah sebagai berikut :

a. Serangan yang digunakan adalah serangan DOS (Denial of Service) yaitu Ping of Death dan Smurf.
b. Dalam klasifikasi akan menggunakan beberapa atribut dari dataset KDD CUP 1999 yaitu duration, protocol_type, service, src_byte, urgent, count, srv_count dan class.
c. Melakukan klasifikasi serangan dengan metode decision tree C4.5.
d. Menggunakan algoritma j48 yang ada pada WEKA, sebagai implementasi decision tree C.45

e. Melakukan analisa terhadap hasil klasifikasi dataset yang dibuat untuk mengetahui keakuratan decision tree dalam mengklasifikasi serangan DOS.

1.4 TUJUAN TUGAS AKHIR

Adapun tujuan dari tugas akhir ini adalah :

a. Mengimplementasikan teknik data mining untuk mengklasifikasikan sebuah serangan DOS.
b. Mengklasifikasikan serangan DOS Ping of Death dan Smurf dengan metode decision tree

1.5 MANFAAT TUGAS AKHIR

Manfaat yang di peroleh dari tugas akhir ini adalah :

a. Dapat melakukan klasifikasi terhadap dataset yang dibuat.
b. Dapat mengetahui tingkat akurasi dari metode decision tree dalam mengklasifikasikan serangan pada dataset yang dibuat.

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan tugas akhir ini akan membantu memberikan informasi tentang tugas akhir yang dijalankan dan agar penulisan laporan ini tidak menyimpang dari batasan masalah yanga ada, sehingga susunan laporan ini sesuai dengan apa yang diharapkan. Sistematika penulisan laporan tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi mengenai gambaran umum penelitain tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan tugas akhir, manfaat tugas akhir, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Tinjauan pustaka berisi tentang berbagai konsep dasar penyerangan, data mining serta analisa yang digunakan dan teori-teori yang berkaitan dengan topik masalah yang diambil dan hal-hal yang berguna dalam proses analisis permasalahan.

BAB III METODE PENELITIAN

Metode tugas akhir ini berisi tentang rancangan jaringan, rancangan serangan-serangan, rancangan klasifikasi, dan konfigurasi-konfigurasi yang digunakan dalam mendeteksi, serta metode-metode lain yang digunakan untuk menyelesaikan tugas akhir ini.

BAB IV HASIL DAN PEMBAHASAN

Dalam implementasi sistem ini berisi tentang hasil dan pembahasan tentang beberapa konfigurasi yang dilakukan pada bab sebelumnya untuk memproses data log mentah TCPdump, serta di lakukannya analisa klasifikasi dataset TCPdump sebagai data test dan menggunakan dataset KDD CUP 1999 sebagai data training menggunakan metode Decion tree dalam melakukan proses klasifikasi.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan dan saran dari penulis yang sudah diperoleh dari hasil penulisan tugas akhir.